

Politique de Certification achatpublic.com

Version 1.0

1	Préambule	3
1.1	Glossaire et bibliographie	3
1.2	Introduction	3
1.3	Politique de Certification	3
2	Les services d'achatpublic.com	3
2.1	Le besoin de confidentialité	3
2.2	L'Autorité de Certification achatpublic.com	3
2.3	Le processus de chiffrement de la Salle des Marchés.	4
2.4	Format de chiffrement	6
3	Règles de gestion du cycle de vie des certificats	6
3.1	Intervenants et applications	6
3.1.1	L'Autorité de Certification	6
3.1.2	L'Autorité d'Enregistrement	7
3.1.3	L'Opérateur de Certification	7
3.1.4	Le Porteur de Certificat	7
3.1.5	L'Utilisateur de Certificat	7
3.1.6	Les types d'applications et les fournisseurs de services	7
3.2	Obligations	8
3.2.1	Obligations de l'AC	8
3.2.2	Obligations de l'OC	8
3.2.3	Obligations de l'AE	9
3.2.4	Obligations du Porteur de Certificat	9
3.2.5	Obligations des Utilisateurs de Certificats	9
3.2.6	Obligations du Fournisseur de Service	9
3.3	Processus du cycle de vie des certificats	10
3.3.1	Attribution de certificat	10
3.3.2	Séquestre et recouvrement	10
3.3.3	Révocation	10
3.3.4	Renouvellement	11
3.4	Profil des certificats	11
3.4.1	Certificat racine d'achatpublic.com	11
3.4.2	Nommage	11
3.4.3	Durée de vie	12
3.4.4	Type de bi-clefs	12
3.4.5	Extensions	12
3.5	Sécurité physique de l'ICP	12
3.6	Contacts et organisation dédiée à la PC	13
3.6.1	Organisation dédiée à la PC	13
3.6.2	Contact	13
3.7	Dispositions applicables et règlement des litiges	13
3.7.1	Dispositions applicables	13

3.7.2	Loi applicable et résolution des litiges	13
3.8	Modifications des spécifications et des composantes de l'AC	13

1 Préambule

1.1 Glossaire et bibliographie

Un glossaire et une bibliographie recensant les termes employés dans le présent document ainsi que les ouvrages de référence cités seront trouvés dans le document *Achatpublic.com-Politiques de Sécurité-Annexes.pdf*.

1.2 Introduction

Le présent document constitue la Politique de Certification (PC) d'achatpublic.com. Il expose dans un premier temps (paragraphe 2) le contexte d'utilisation des certificats de chiffrement délivrés par achatpublic.com, et dans un deuxième temps (paragraphe 3) les pratiques appliquées par achatpublic.com, en qualité d'Autorité de Certification (AC), lors de l'émission, la gestion du cycle de vie et la publication de ces certificats de chiffrement.

1.3 Politique de Certification

Lorsqu'une Autorité de Certification (AC) émet un Certificat, elle indique de ce fait à l'Utilisateur de Certificat qu'une clef publique spécifique est associée à un Porteur de Certificat spécifique identifié par le sujet du Certificat. Un Certificat peut être émis selon des pratiques et des procédures différentes, et peut convenir à des applications et/ou des fins diverses.

Et, conformément à [RFC 3280], une Politique de Certification (PC) constitue un ensemble nommé de règles qui prescrivent l'applicabilité d'un Certificat à une collectivité et/ou à une classe d'applications particulières ayant des exigences communes en matière de sécurité.

En conséquence et compte tenu de la grande importance des PC pour établir la confiance à l'égard d'un Certificat, il est primordial que la présente PC soit bien comprise et soit consultée non seulement par les Porteurs de Certificat, mais également par tout Utilisateur de Certificat.

L'attention du lecteur est attirée sur le fait que la compréhension de la présente PC suppose que le lecteur soit familiarisé avec les notions liées à la technologie des Infrastructures à Clefs Publiques (ICP).

2 Les services d'achatpublic.com

La société achatpublic.com commercialise un service de dématérialisation des procédures de passation des marchés publics. A ce titre, elle met à disposition de ses clients et usagers une plate-forme accessible sur Internet via l'adresse <http://www.achatpublic.com>, comprenant notamment une « Salle des Marchés », dans laquelle se réalisent les échanges sécurisés de données dans le cadre des procédures de passation de marchés publics décrites par le Code des marchés publics.

2.1 Le besoin de confidentialité

Le Code des Marchés Publics impose que les plis remis par les soumissionnaires bénéficient d'une garantie de confidentialité. C'est pourquoi un chiffrement de bout en bout des plis remis est effectué : les plis sont chiffrés sur le poste du soumissionnaire avant émission, et ne sont déchiffrés qu'en séance par la personne habilitée au sein de la collectivité publique.

2.2 L'Autorité de Certification achatpublic.com

achatpublic.com délivre, dans le cadre exclusif du fonctionnement de la Salle des Marchés, des certificats et bi-clefs servant au chiffrement et au déchiffrement des plis des soumissionnaires.

Ces éléments ne sont qu'un maillon de la chaîne de confidentialité.

Les pratiques et contraintes appliquées à la délivrance de ces certificats sont adaptées au niveau de criticité de la fonction remplie. Ces certificats sont utilisés dans le cadre d'un service, et remplissent plus un rôle fonctionnel qu'un rôle de sécurité à proprement parler.

2.3 Le processus de chiffrement de la Salle des Marchés.

Etape 1 : Lors de la souscription au service : fourniture par achatpublic.com à la Collectivité Publique de **clefs de déchiffrement**. Ce processus de délivrance est décrit au paragraphe 3.2.6. La Collectivité Publique dispose d'un ou plusieurs exemplaires identiques de sa clef de déchiffrement. Ces clefs se présentent sous la forme de cartes à puces, de clefs USB ou de fichiers au format PKCS#12 / CMS tel que décrit dans [RFC 2630]. La Personne Publique demeure libre d'attribuer ces clefs de déchiffrement au sein de son organisation afin d'assurer la bonne tenue des commissions d'ouverture des plis.

La clef publique correspondante est conservée par achatpublic.com pour transmission aux soumissionnaires, qui devront s'en servir pour constituer leurs plis.

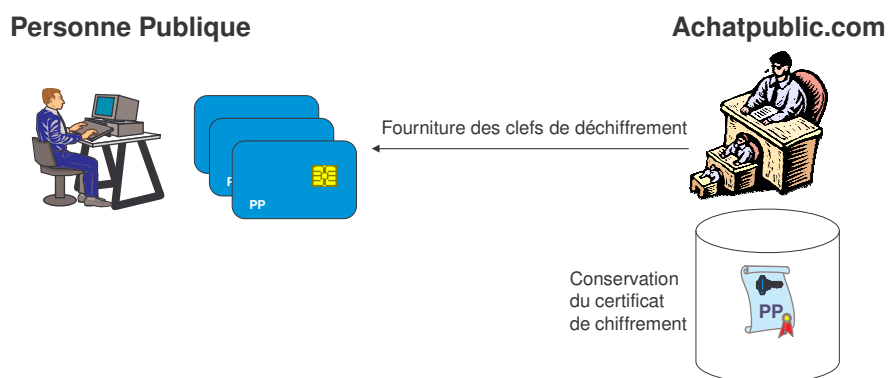


Figure 1 : Fourniture des clefs de déchiffrement

Etape 2 : Chiffrement des plis par le soumissionnaire. Le soumissionnaire, une fois ses plis constitués, doit en réaliser le chiffrement avant de les envoyer.

Le chiffrement de données est un mécanisme à deux étapes :

- les données sont d'abord chiffrées avec un algorithme symétrique, à l'aide d'une clef à usage unique K générée explicitement pour le présent chiffrement et changeant à chaque nouveau chiffrement ;
- puis cette clef K est elle-même chiffrée à l'aide d'un algorithme asymétrique, avec la clef publique du destinataire (la Personne Publique), qui est extraite de son certificat.

Il est à noter que le chiffrement est réalisé automatiquement et de manière quasi-invisible, seul un suivi d'avancement de l'opération étant affiché. Par souci de simplicité, aucune action et aucun contrôle ne sont demandés à l'entreprise soumissionnaire. C'est la base de certificats de la plate-forme achatpublic.com qui est garante de la validité des certificats utilisés pour le chiffrement.

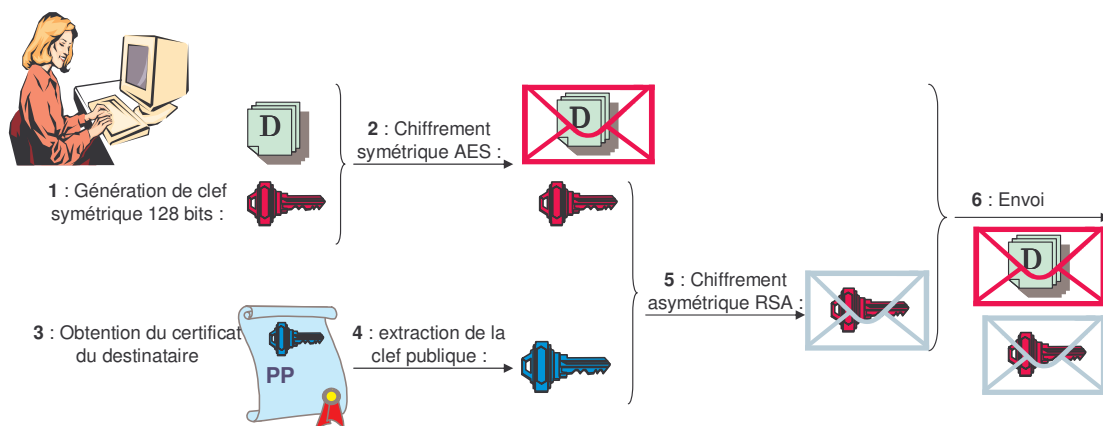


Figure 2 : Le chiffrement des données

Ainsi, pour accéder à un document en clair, il faut disposer de trois éléments :

- i. le document chiffré par un algorithme symétrique (en l'espèce : AES) à l'aide de la clef K ;
- ii. la clef symétrique K elle-même chiffrée par la clef publique de la Personne Publique ;
- iii. La clef privée de la Personne Publique, qui lui a été délivrée lors de l'étape 1.

Etape 3 : Téléchargement des plis par la Personne Publique. Afin de préparer la commission d'ouverture des plis, la Personne Publique télécharge, préalablement à sa tenue, les plis chiffrés. De cette manière, aucun téléchargement de données lourdes n'aura lieu en cours de Commission, tous les documents volumineux étant préalablement présents sur le poste de travail.

A cette étape, la Personne Publique dispose des éléments i et iii mais pas de l'élément ii, et ne peut donc pas accéder aux documents en clair.

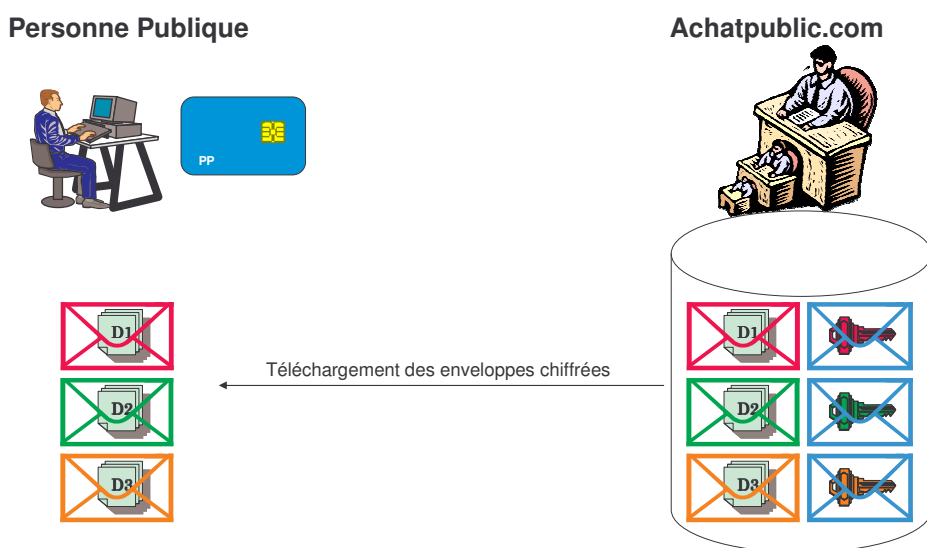


Figure 3 : Téléchargement des plis chiffrés avant la Commission

Etape 4 : Ouverture des plis par la Personne Publique. Lors de la commission d'ouverture des plis, la Personne Publique détermine selon ses critères quels plis doivent être déchiffrés. Cette action est régie par une habilitation particulière au sein du service Salle des Marchés. Seules les clefs relatives à ces plis admis sont téléchargées.

Dès le téléchargement de la clef - élément ii -, la Personne Publique est en possession des trois éléments lui permettant de réaliser le déchiffrement du pli. C'est donc dès le téléchargement de l'élément ii que le pli est réputé ouvert. L'opération de déchiffrement proprement dite, impliquant les éléments i, ii et iii tous trois présents sur le poste, n'est alors qu'une opération technique, qui n'a pas de sens juridique dans le cadre de la procédure.

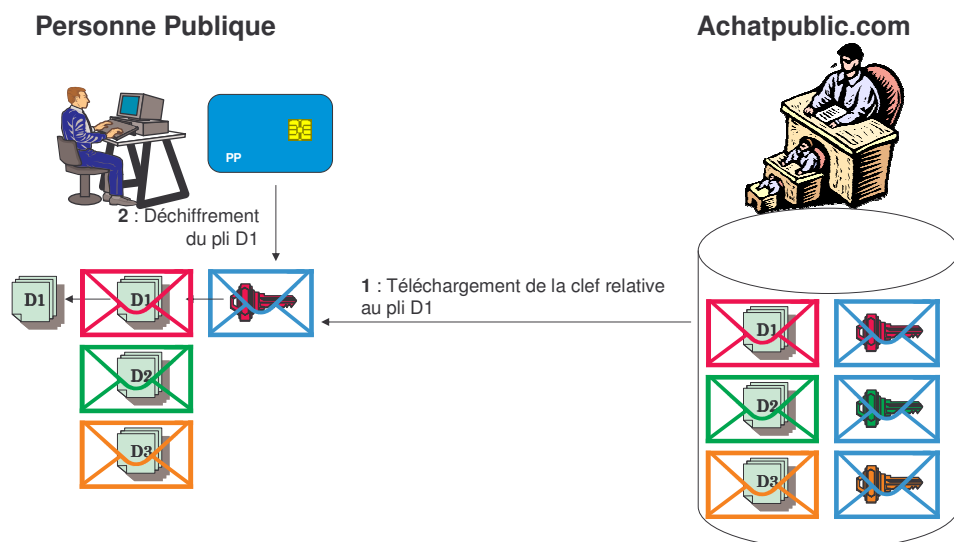


Figure 4 : Ouverture des plis

Étape 5 : Preuve de suivi d'ouverture de plis. A l'issue de la procédure, achatpublic.com délivre une liste, horodatée, des éléments ii téléchargés, pli par pli. Cette liste, nommée « preuve de suivi d'ouverture des plis », fait foi des plis ouverts ou non ouverts. Les plis pour lesquels l'élément ii n'a pas été téléchargé sont réputés non ouverts.

En résumé :

Le chiffrement permet la confidentialité essentielle au service. L'utilisation des certificats est réalisée de manière invisible pour l'entreprise soumissionnaire, entièrement sous le contrôle du service achatpublic.com. Le déchiffrement est soumis au téléchargement des clés, qui est réalisé dans un contexte de contrôle d'habilitations. Le déchiffrement n'a pas un rôle de sécurité mais un rôle fonctionnel.

2.4 Format de chiffrement

Le standard de chiffrement employé sur Internet est CMS, décrit dans [RFC 2630].

L'algorithme de chiffrement symétrique est AES avec des clés de 128 bits.

L'algorithme de chiffrement asymétrique est RSA avec des clés de 1024 bits.

Les données chiffrées et les clés sont stockées dans deux fichiers au format CMS distincts, de manière à permettre le téléchargement indépendant des données chiffrées et des clés de déchiffrement.

3 Règles de gestion du cycle de vie des certiactifs

3.1 Intervenants et applications

3.1.1 L'Autorité de Certification

L'AC est responsable de l'ensemble de l'Infrastructure à Clef Publique qu'elle a mis en place. Pour les Certificats signés en son nom, l'AC assure les fonctions suivantes :

- Gestion de l'ensemble de l'Infrastructure à Clef Publique qu'elle a mise en place,
- Mise en application de la présente PC,
- Emission des Certificats,
- Gestion de la révocation des certificats,
- Gestion des Certificats.

L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité.

3.1.2 L'Autorité d'Enregistrement

achatpublic.com joue à la fois le rôle d'AC et d'AE. Les fonctions suivantes sont constitutives du rôle d'AE :

- Gestion des demandes de Certificats,
- Vérification de l'identité du Porteur de Certificat,
- Enregistrement des Porteurs de Certificats,
- Information du Porteur de Certificat sur les contraintes liées à l'usage d'un Certificat,
- Archivage des dossiers de demandes de Certificats,
- Vérification des demandes de Révocation de Certificats.

3.1.3 L'Opérateur de Certification

L'OC est responsable vis-à-vis de l'AC de l'exploitation technique du service de génération des certificats et de leur acheminement vers les Porteurs de Certificats. Ses rôles sont les suivants :

- Garantir la sécurité des clefs racines,
- Recevoir les demandes de certificats,
- S'assurer du bon format de ces demandes,
- Procéder à la génération des certificats dans les conditions prévues par la présente PC,
- Séquestrer les clefs privées et les certificats,
- Recevoir les demandes de recouvrement,
- Procéder au recouvrement des certificats dans les conditions prévues par la présente PC,
- Expédier les bi-clefs et certificats (générés ou recouverts) d'une part, et les données d'activation d'autre part, directement aux Porteurs de Certificats, par deux canaux différents.

achatpublic.com délègue le rôle d'Opérateur de Certification à un tiers de manière à ne pas disposer des clefs privées de déchiffrement, qui sont générées uniquement à l'attention des Porteurs de Certificats.

3.1.4 Le Porteur de Certificat

Les certificats délivrés par achatpublic.com ne sont pas nominatifs. Ils sont en revanche propre aux Collectivités Publiques clientes du service Salle des Marchés d'achatpublic.com.

Le Porteur de Certificat est la Collectivité Publique cliente d'achatpublic.com. Ses responsabilités sont les suivantes :

- Conserver secrète la clef privée,
- Conserver secrètes les données d'activation,
- Désigner en son sein la ou les personnes physiques qui seront les utilisateurs légitimes du certificat et les modalités d'utilisation (dans le cadre du service « salle des marchés » d'achatpublic.com),
- Utiliser le certificat uniquement pour les services définis dans la présente PC et conformément à l'usage défini par l'AC.

3.1.5 L'Utilisateur de Certificat

L'Utilisateur de Certificat est toute personne qui utilise un certificat de chiffrement pour chiffrer des données à l'attention du Porteur de Certificat. Il est de la responsabilité de l'Utilisateur de Certificat de n'utiliser ce certificat que dans le cadre applicatif défini par la présente Politique de Certification et par les Conditions Générales d'Utilisation des services d'achatpublic.com.

3.1.6 Les types d'applications et les fournisseurs de services

Il est expressément entendu que la présente PC n'autorise l'utilisation des Certificats émis en vertu de cette PC qu'à des fins de chiffrement de données à l'attention du Porteur de Certificat et de déchiffrement de ces données par ledit Porteur.

Fournisseurs de service

Le fournisseur de service est l'entité qui fournit un service nécessitant l'usage des Certificats. Un tel service est appelé Application. Une Application cible est une application dans le cadre de laquelle l'usage des Certificats émis

au titre de la présente PC est autorisé. Le seul Fournisseur de service habilité à employer les certificats émis au titre de la présente PC au sein de l'Application qu'il fournit est achatpublic.com.

Application cible

La seule Application cible est la Salle des Marchés d'achatpublic.com, et au sein de ce service, seule la fonction de chiffrement et de déchiffrement.

Applications hors cibles

Il s'agit de toute Application qui ne figure pas dans la liste des Applications cibles.

L'Autorité de Certification achatpublic.com ne saurait être responsable de l'utilisation d'un Certificat dans le cadre d'une Application hors cible. Etant rappelé que tout Utilisateur a, conformément aux usages en la matière, l'obligation d'identifier et contrôler la PC en vertu de laquelle le Certificat qu'il utilise est émis, et en particulier la liste des applications cibles.

3.2 Obligations

3.2.1 Obligations de l'AC

L'AC s'engage à mettre en œuvre les moyens décrits dans la présente PC afin de permettre d'assurer :

- La qualité et sécurité des prestations auxquelles elle s'engage,
- La définition d'un cadre contractuel entre elle et chaque Porteur de Certificat par lequel notamment seront définis les droits et obligations de l'AC et du Porteur de Certificat concerné,
- Le respect des dispositions contractuelles susvisées,
- L'utilisation de sa clef privée de signature de Certificat aux seules fins de signature des Certificats et des LCR,
- La protection de ses clefs privées et ses Données d'Activation.

3.2.1.1 S'agissant des fonctions de gestion des Certificats

L'AC s'engage à mettre en œuvre les moyens décrits dans la présente PC afin de permettre d'assurer :

- L'émission et la délivrance du Certificat au Porteur de Certificat,
- La conformité des informations contenues dans le Certificat avec les informations recueillies aux fins de délivrance de Certificats,
- La mise en œuvre des procédures de Renouvellement des Certificats conformément à la présente PC,
- La mise en œuvre des procédures de Révocation des Certificats conformément à la présente PC.

3.2.1.2 S'agissant de la fonction de publication

L'AC s'engage à mettre en œuvre les moyens décrits dans la présente PC afin de permettre d'assurer la publication et l'accès à la présente Politique de Certification.

3.2.1.3 S'agissant de la fonction de séquestre

L'AC s'engage à mettre en œuvre les moyens décrits dans la présente PC afin de permettre d'assurer :

- Le séquestre des bi-clefs et certificats de déchiffrement dans des conditions assurant leur confidentialité,
- Le recouvrement des bi-clefs et certificats de déchiffrement par leurs Porteurs de Certificats.

L'AC s'engage à ne jamais procéder, ou faire procéder par l'OC, pour son propre compte ou pour le compte d'un tiers autre que le Porteur de Certificat, de recouvrement ou de copie de bi-clef de déchiffrement.

3.2.2 Obligations de l'OC

L'OC s'engage à ne transmettre les bi-clefs et certificats émis au titre de la présente PC qu'aux seuls destinataires dont les coordonnées ont été transmises par l'AC dans les requêtes de certification ou de recouvrement.

L'OC s'engage à ne jamais procéder, pour son propre compte ou pour le compte d'un tiers autre que le Porteur de Certificat, de recouvrement ou de copie de bi-clef de déchiffrement.

3.2.3 Obligations de l'AE

L'AE s'engage à mettre en œuvre les moyens décrits dans la présente PC afin de permettre d'assurer :

- La vérification de la compatibilité des informations recueillies avec celles exigées par la présente PC pour la délivrance de Certificats,
- La conformité des informations contenues dans le Certificat avec les informations recueillies aux fins de délivrance de Certificats,
- La vérification de l'authenticité d'une demande de Révocation qui lui est soumise conformément à la présente PC,

3.2.4 Obligations du Porteur de Certificat

L'AC est liée contractuellement avec chaque Porteur de Certificat (Collectivité Publique) pour l'émission de Certificats.

Le Porteur de Certificat est responsable des obligations ci-après mentionnées :

- Garantir l'authenticité, le caractère complet et à jour des informations communiquées lors de la demande de Certificat ainsi que des documents qui accompagnent ces informations,
- Informer sans délai l'AE et l'AC de toute modification relative à ces informations et/ou documents,
- Assurer l'information des personnes mandatées pour l'utilisation des certificats dans le cadre des Applications Cibles sur les conditions d'utilisation des Certificats, de la gestion des clefs ou encore de l'équipement et des logiciels permettant de les utiliser,
- Faire protéger la clef privée de chaque Certificat par des moyens appropriés à son environnement,
- Faire protéger les Données d'Activation de chaque Certificat par des moyens appropriés à leur environnement,
- Faire respecter les conditions d'utilisation de la clef privée et du Certificat correspondant, notamment l'utilisation dans le strict cadre des applications décrites par la présente PC,
- Faire demander la Révocation d'un Certificat dès lors qu'elle est nécessaire,
- Faire informer sans délai l'AE ou l'AC en cas de compromission ou de suspicion de compromission de la clef privée.

3.2.5 Obligations des Utilisateurs de Certificats

Pour permettre une utilisation d'un Certificat, dans des conditions optimales de sécurité, il est rappelé que l'Utilisateur doit :

- Avoir pris connaissance de la PC en vertu de laquelle le Certificat qui lui est adressé est émis afin de lui permettre notamment :
 - de refuser un Certificat qui ne serait pas utilisé conformément à la présente PC et notamment qui serait utilisé hors du champ des Applications cibles définies par la présente PC,
 - de vérifier l'objet pour lequel le Certificat est émis. Dans le cadre de la présente PC, le Certificat ne garantit que l'Identité du Porteur de Certificat,
- Contrôler ou avoir connaissance de la validité de la signature électronique de l'AC émettrice du Certificat,
- Contrôler la validité des Certificats en vérifiant la date de validité du Certificat et la LCR, afin de lui permettre de refuser tout Certificat révoqué ou ayant expiré.

L'AC n'est pas responsable des conséquences dommageables qui seraient dues au non respect par les Utilisateurs des contrôles ci-dessus rappelés.

3.2.6 Obligations du Fournisseur de Service

En tant que fournisseur du service Salle des Marchés, achatpublic.com s'engage à publier dans l'annuaire les certificats de chiffrement des collectivités publiques clientes du service de manière à les rendre utilisables par les entreprises soumissionnaires dans le cadre du service.

Le fournisseur du service s'engage à ne pas ajouter, à ce certificat et aux certificats de chiffrement que la collectivité publique y aurait ajoutés, d'autres certificats permettant à elle-même ou à un tiers d'avoir la capacité de déchiffrer les clefs de chiffrement symétriques.

3.3 Processus du cycle de vie des certificats

3.3.1 Attribution de certificat

L'attribution d'un certificat fait partie du processus d'inscription pour l'accès au service Salle des Marchés d'achatpublic.com.

Les informations relatives à l'identité de la collectivité publique cliente, qui devient le Porteur du Certificat, sont recueillies lors de ce processus.

Lorsqu'une collectivité publique crée dans le cadre du service Salle des Marchés une sous-entité gérant ses marchés indépendamment, elle doit procéder à une nouvelle demande de certificat pour cette entité.

Les informations recueillies pour la génération d'un certificat sont :

- le nom de la collectivité publique et, dans le cas d'une sous-entité, le nom de toutes les sous-entités de niveau supérieur à l'entité qui devient le Porteur de Certificat ;
- l'adresse de livraison du certificat ;
- le type de support, au choix :
 - carte à puce
 - clef USB ;
 - logiciel (livré sur disquette) ;
- le nombre de supports identiques demandés.

Ces informations sont transmises à l'Opérateur de Certification, ainsi que les Données d'Activation, générées par l'AC.

La bi-clef et le Certificat sont générés, inscrits sur les supports et séquestrés par l'Opérateur de Certification. L'Opérateur de Certification effectue l'envoi des supports au Porteur de Certificat, à l'adresse indiquée par l'AC dans la requête.

L'Opérateur de Certification effectue l'envoi des Données d'Activation de ces supports au Porteur de Certificat.

Les supports et donc les clefs privées ne sont jamais connues de l'AC.

3.3.2 Séquestre et recouvrement

Les bi-clefs et certificats sont séquestrés par l'Opérateur de Certification de manière sécurisée.

Le recouvrement se fait par le même processus que l'émission d'origine, la demande précisant qu'il s'agit d'un certificat préexistant et non d'une génération de nouveau certificat.

3.3.3 Révocation

Lorsque l'une des circonstances ci-dessous se produit, le Certificat concerné doit être révoqué et inscrit dans la LCR ; il cesse également d'être utilisé dans le cadre de l'application « Salle des Marchés » d'achatpublic.com :

- Changement dans les informations et/ou documents communiqués lors de la demande de Certificat avant l'expiration normale du Certificat,
- Non respect par le Porteur de Certificat des modalités applicables à l'utilisation du Certificat,
- Perte, vol, compromission ou suspicion de compromission de la clef privée associée à la clef publique certifiée,
- Demande de Révocation émanant du Porteur de Certificat,
- Révocation du Certificat de l'AC (ce qui entraîne la Révocation des Certificats signés par la clef privée correspondante),
- Cessation d'activité du Porteur de Certificat,
- Evolution de l'état de l'art cryptographique : par exemple lorsque la taille des clefs ou les algorithmes de chiffrement deviennent obsolètes. Les Certificats concernés doivent être révoqués,
- Il a été démontré une fraude dans le dossier de demande de Certificat.

La demande de révocation doit se faire par courrier auprès de l'entité désignée au paragraphe 3.6. Elle sera suivie d'une vérification téléphonique.

La révocation sera effective lorsque le certificat incriminé aura été retiré de la base de certificats utilisés par l'application Salle des Marchés d'achatpublic.com. En effet, cette application ne gère pas de LCR pour les certificats de chiffrement, et les certificats de chiffrement n'étant utilisés que dans le cadre de cette seule application, il est inutile de diffuser la LCR.

3.3.4 Renouvellement

Le renouvellement est systématique et ne nécessite pas de demande de la part du Porteur de Certificat. Il s'effectue de la même manière que l'émission d'origine.

3.4 Profil des certificats

Les Certificats produits par l'AC sont conformes au standard ITU-T Recommandation X.509 repris dans [RFC 3280].

3.4.1 Certificat racine d'achatpublic.com

Les certificats de chiffrement d'achatpublic.com sont émis par le certificat racine d'achatpublic.com. Ce certificat racine est décrit par les éléments suivants :

Numéro de série : 0

Emetteur :

- CN = ACHATPUBLIC.COM
- O = ACHATPUBLIC.COM
- C = FR

Validité : du jeudi 3 juin 2004 17:51:58 au jeudi 24 mai 2007 17:51:58

Objet :

- CN = ACHATPUBLIC.COM
- O = ACHATPUBLIC.COM
- C = FR

Clef publique RSA 2048 bits :

```
30 82 01 0a 02 82 01 01 00 98 5d 31 ae bc 83 07 ee 29 c3 e7 e3 48 6f 2b 26 60 47 f2 7e
d0 1d 21 6b 5d 58 e9 67 ae fe ec c9 8f 0b d9 23 0e a3 34 90 5d ae 74 f6 26 a9 d5 bc 5d
d3 a5 e7 dc d3 ec a2 2c 61 6d 0d f4 fa 54 16 94 86 de a1 ed d5 60 5e 89 13 f8 05 ca 6d
78 e0 31 5a 2a 8f 82 cb 33 c0 43 bd 8d 3d c5 6f 74 b9 9a e7 ac 3a e0 a4 64 16 ad 94 8f
c4 b4 a7 aa 0b 00 23 53 a3 0c 70 d9 ce 77 01 a4 f9 8c 22 86 19 38 80 5d 40 d7 c8 a1 63
9c 85 4d 56 55 8d 4b 17 05 fd cb d7 92 fc 3f 07 6b 47 d7 bd cf 63 10 ad ea 6e a3 f5 35
55 15 83 70 32 2f 36 7c e7 d1 ab 25 f7 11 cc d3 35 b7 44 34 96 e5 2a 4a 90 7e fd 92 2c
8b 6f 96 81 61 5f ae a9 bb 92 fc 77 eb 1d d2 fa 08 b4 39 7c 27 f3 36 47 fa 85 56 36 92
3e 19 93 44 28 1c e6 47 8b a0 cc 60 66 69 82 d2 0c 5e 8d 8d cb 7b 17 00 fa fa e3 d3 3f
e9 3f 3e 71 02 03 01 00 01
```

Identificateur de la clef du sujet :

```
ac 44 ed 42 9c 63 77 1f 0f a9 ba c0 f2 2a 60 4b db 14 55 81
```

Algorithme d'empreinte numérique : SHA1

Empreinte numérique :

```
12 9b 9f 71 67 31 93 ac 8c f0 29 96 c9 a6 21 63 42 f6 19 f9
```

3.4.2 Nommage

Chaque Certificat a un nom distinctif (DN) unique. Ce DN est un nom de type X.501 et est encodé en printableString ou en UTF8String, et est présent dans le champ *Subject* du Certificat.

Le champ *Subject* du Certificat est composé du DN comme suit :

c = FR

o = ACHATPUBLIC.COM

cn = nom d'affichage du porteur du certificat tel que défini dans l'application achatpublic.com

Dans le cas où le porteur du certificat est une sous-entité d'une collectivité, le cn est constitué de la manière suivante :

Nom d'affichage de la collectivité – Noms d'affichage des collectivités supérieures dans l'ordre ascendant.

Le cn est limité à 100 caractères.

3.4.3 Durée de vie

La durée de vie des certificats est de trois ans.

3.4.4 Type de bi-clefs

Les bi-clefs associées aux certificats sont de type RSA 1024 bits.

3.4.5 Extensions

Les Certificats de chiffrement émis par l'AC contiennent les champs primaires et les extensions suivantes :

Champ	Explications
Version	Version du Certificat X.509 (v3)
Numéro de série	Le numéro de série unique du Certificat
Algorithme de signature	Identifiant de l'algorithme de signature de l'AC (SHA-1WithRSA)
Emetteur	Le nom de l'AC émettrice est le Distinguished Name (X.500) de l'AC signant les Certificats
Valide à partir du Valide jusqu'au	Dates et heures d'activation et d'expiration du Certificat
Objet	Nom distinctif de l'entité identifiée
Clef publique	Identifiant de l'algorithme d'usage de la clef publique contenue dans le Certificat, et valeur de la clef publique
Commentaire Netscape	permet un affichage dans certains navigateurs
AuthorityKeyIdentifier	Identifie la clef publique utilisée pour vérifier la signature sur un Certificat
SubjectKeyIdentifier Identifier	Identifie la paire de clef dont la clef publique est contenue dans la clef
Key Usage	keyEncipherment
Contrainte de base	SubjectType = EndEntity ; PathLengthConstraint = None Indique qu'il s'agit d'un Certificat de Porteur et non d'AC
Algorithme d'empreinte numérique	SHA-1
Empreinte numérique	Champ d'octets caractérisant le Certificat de l'AC ayant signé le Certificat

3.5 Sécurité physique de l'ICP

Des contrôles sont effectués sur les équipements de l'OC, sur les points suivants :

- Situation géographique et construction de sites,
- Accès physique,
- Energie et air conditionné,
- Exposition aux liquides,
- Sécurité incendie,
- Conservation des médias.

L'ICP est exploitée hors-ligne, sans aucun contact avec Internet ou tout autre réseau public.

achatpublic.com s'engage à exploiter les clefs privées nécessaires au service de validation de certificats selon les pratiques de l'état de l'art relatif à l'exploitation de tels services.

achatpublic.com s'engage à être auditable de manière à pouvoir fournir une mesure objective de la qualité de la gestion de ses clefs privées.

3.6 Contacts et organisation dédiée à la PC

3.6.1 Organisation dédiée à la PC

achatpublic.com est responsable de l'élaboration, du suivi et de la modification dès que nécessaire de la présente PC. A cette fin elle a mis en œuvre une organisation dédiée coordonnée par un Responsable de la Certification. L'organisation dédiée statue sur toute modification nécessaire à apporter à la PC.

3.6.2 Contact

Le Responsable de la Certification est le seul contact habilité vis-à-vis des organisations extérieures à achatpublic.com.

Coordonnées :

achatpublic.com

M. le Responsable de la Certification

107, avenue Parmentier

75011 Paris

3.7 Dispositions applicables et règlement des litiges

3.7.1 Dispositions applicables

Il est expressément entendu qu'en l'état de la pratique et des textes législatifs et réglementaires en vigueur, les Certificats émis en vertu de la présente PC sont des Certificats simples dont les conditions d'utilisation sont définies par la présente PC et/ou par le contrat d'abonnement aux services de certification définissant les relations entre l'AC et un Porteur de Certificat.

La présente PC est susceptible d'être adaptée, si nécessaire, en fonction de toute évolution législative et réglementaire qui pourra avoir un impact sur les conditions d'émission, de gestion des Certificats ou sur les obligations respectives des intervenants.

Les relations entre l'AC d'une part et les Porteurs de Certificats d'autre part sont régies par un contrat d'abonnement au service de certification entre l'AC et le Porteur de Certificat et par les dispositions de la présente PC.

Les relations entre l'AC et l'Utilisateur sont régies par les dispositions de la présente PC et les Conditions Générales d'Utilisation des services d'achatpublic.com.

3.7.2 Loi applicable et résolution des litiges

La présente PC est soumise au droit français.

Tout litige relatif à la validité, l'interprétation, l'exécution de la présente PC sera soumis aux tribunaux de la cour d'appel de Paris.

3.8 Modifications des spécifications et des composantes de l'AC

L'AC procède à toute modification des spécifications stipulées dans la PC et/ou des composantes de l'IGC qui lui apparaît nécessaire pour l'amélioration de la qualité des services de Certification et de la sécurité des processus.

L'AC procède également à toute modification des spécifications stipulées dans la PC et/ou des composantes de l'AC qui est rendue nécessaire par une législation ou réglementation en vigueur.

L'AC informera les Applications cibles et/ou les Porteurs de telles modifications dès lors qu'il s'agit de modifications majeures ayant un impact déterminant.

L'information sera effectuée par l'AC par tout moyen, notamment à l'aide de message électronique spécifique, en respectant, dès lors que cela est possible, un préavis raisonnable avant l'entrée en vigueur des modifications.